



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/027,622	12/19/2001	Kenneth W. Aull	NG(MS)7194	2941
26294 7590 06/29/2007 TAROLLI, SUNDHEIM, COVELL & TUMMINO L.L.P. 1300 EAST NINTH STREET, SUITE 1700 CLEVEVLAND, OH 44114			EXAMINER KHOSHNOODI, NADIA	
			ART UNIT 2137	PAPER NUMBER
			MAIL DATE 06/29/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

MAILED

Application Number: 10/027,622
Filing Date: December 19, 2001
Appellant(s): AULL ET AL.

JUN 29 2007

Technology Center 2100

Christopher P. Harris
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 3/5/2007 appealing from the Office action
mailed 11/27/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,192,131	Geer, Jr. et al.	02-2001
6,615,171	Kanevsky et al.	09-2003
2003/0005291	Burn	01-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-6, 8-14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geer, Jr. et al., United States Patent No. 6,192,131, and further in view of Kanevsky et al., United States Patent No. 6,615,171.

As per claims 1 and 9:

Geer, Jr. et al. teach a method comprising: accessing the token through a token reader connected to a computer system by a certificate authority (col. 2, lines 27-39); reading a user signature certificate from the token (col. 2, lines 51-60); creating a certificate and an associated private key and digitally signing the certificate and the associated private key using a signature certificate of the certificate authority (col. 9, lines 24-41); downloading the certificate and the associated private key to the token (col. 6, lines 15-27); and decrypting the certificate and the associated private key to the token, such that the token stores at least the private key, the user signature certificate and the certificate and the associated private key (col. 4, lines 15-25 and col. 6, lines

15-27).

Not explicitly disclosed is reading a token ID and searching for a match for the token ID and the signature certificate in an authoritative database and wherein the certificate and the associated private key are wrapped with a public key associated with the token ID if a match for the token ID and the user signature certificate is found in the authoritative database. However, Kanevsky et al. teach that the token ID and certificate as supplied by the user's smart card are searched for in a database to determine whether or not a valid user is attempting to gain access to the system. Furthermore, Kanevsky et al. teach that once a user is identified as being valid, the encryption can occur. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Geer, Jr. et al. to incorporate the ability to determine that the users are who they say they are by checking a database for the token ID and certificate information supplied by the users' smart card and to allow other steps, such as for encryption to occur only when a match is found. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Kanevsky et al. suggest that searching for a match in the database allows one to verify that the user is a valid user to ensure that only valid users ultimately gain access to the resources such as the ability to encrypt the data at hand in col. 8, lines 29-46.

As per claims 2 and 10:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 1 and 9 above. Furthermore, Geer, Jr. et al. teach the method, wherein the

certificate and the associated private key is a plurality of certificates and associated private keys wherein at least one of the plurality of certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user and a role certificate and associated private key for the user wherein the role certificate includes at least one policy (col. 2, lines 51-60 and col.3, lines 29-33).

As per claim 3 and 11:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 2 and 10 above. Furthermore, Geer, Jr. et al. teach the method wherein the wrapping of the certificate and the associated private key with the public key of the token encrypts the certificate and the associated private key (col. 3, lines 16-22).

As per claims 4 and 12:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 3 and 11 above. Furthermore, Geer, Jr. et al. teach the method, wherein the token is a smart card (col. 2, lines 27-36).

As per claims 5 and 13:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 4 and 12 above. Furthermore, Kanevsky et al. teach the method wherein the token ID is assigned by a token manufacturer at the time the token is created and stored in the authoritative database when assigned to a user (col. 7, lines 49-59).

As per claims 6 and 14:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in

claims 5 and 13 above. Furthermore, Geer, Jr. et al. teach the method wherein downloading the certificate and the associated private key to the token is done through an unsecured communications line (col. 11, lines 50-59).

As per claims 8 and 16:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 1 and 9 above. Furthermore, Geer, Jr. et al. teach the method further comprising: authenticating, by the signing of the certificate and associated private key using a signature certificate of the certificate authority, that the certificate and associated private key were issued by the certificate authority (col. 4, lines 4-9).

Claims 7 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geer, Jr. et al., United States Patent No. 6,192,131 and Kanevsky et al., United States Patent No. 6,615,171 as applied to claims 7 and 15 above, and further in view of Burn, United States Pub. No. 2003/0005291.

As per claims 7 and 15:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 6 and 14 above. Not explicitly disclosed is wherein decrypting the certificate and associated private key using the private key stored in the token requires the entry of a pass phrase by a user. However, Burn teaches the method of having a user PIN in order to access the certificate which is what allows access to decrypt messages received, the first of which contains the certificate of the server (fig. 5, elements 140 and 150). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Geer, Jr. et al. to incorporate the

ability to check for a pass phrase entered by the user to allow the decryption to occur. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Burn suggests that adding the step of a user entering a pass phrase ensures that only the user can gain access to the securely encrypted materials so as not to compromise the data on the token in par. 6.

****References Cited, Not Used***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. U.S. Patent No. 6,003,014
2. U.S. Patent No. 6,460,138
3. U.S. Patent No. 5,721,781
4. U.S. Patent No. 5,671,279
5. U.S. Pub. No. 2002/0026578
6. U.S. Pub. No. 2001/0002485

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

(10) Response to Argument

Regarding Claims 1 and 9, 35 USC 103(a) Rejection:

Appellant contends, "Geer in view of Kanevsky does not teach or suggest accessing a token through a token reader connected to a computer system by a certificate authority." Examiner respectfully disagrees. First, the Examiner would like to point out that Geer teaches the use of public key certificates on a smart card (for one example, see col. 5, lines 1-10 and col. 6, lines 6-9). It is also important to note that a signature certificate, since not specifically defined, is nothing more than a certificate that

contains a public key which can be used to verify a digital signature (see MPEP 2111).

With respect to accessing a token through a token reader by a certificate authority, Geer et al. teach that information within a token is accessed via a network by a certifying authority in col. 2, lines 27-39 and Figure 1, elements 10, 12, and 18: *"a system for implementing a transaction in accordance with the present invention includes an **authorizing computer 10, a smart card 12 at authorizing computer 10 that corresponds to a specific user of the authorizing computer 10, an authorized computer 14 that is authorized by authorizing computer 10 to perform some specific action, and a transaction computer 16 that performs a transaction with authorized computer 14 that includes the authorized computer 14 performing the authorized action. The system also includes a certifying authority 18 that performs the conventional function of certifying the identity of the user to authorized computer 14 and transaction computer 16."*** In the previously cited portion, Geer teaches that a certifying authority is necessary to certify the identity of the user to the authorized computer and to the transaction computer. Thus, in order to perform the operations of the invention disclosed by Geer, the certificate authority must have access to the user's information via the smart card, i.e. **the token**, in order to be able to prove the user's identity to the computers that the user is requesting some type of service from. Furthermore, the term **"accessing"** is broad and is therefore broadly interpreted to mean obtaining the user information via a network, according to MPEP 2111. For these reasons, Geer in view of Kanevsky teaches/suggests accessing a token through a token reader connected to a computer system by a certificate authority.

Appellant further contends, "Geer taken in view of Kanevsky does not teach or suggest downloading a certificate and an associated private key to a token." Examiner respectfully disagrees. Geer teaches several different examples of how the system used, one of which uses conversation certificates which are created and downloaded to the user's smartcard with the private key in order to allow for secure communications in col. 9, lines 24-29: "*Referring to FIG. 6, in operation of the system of FIG. 5, **each of the actual parties to the business deal obtains, from a certifying authority computer operated by an investment banking firm, an authorization certificate and a private key of a new public key pair minted by the certifying authority computer (step 78).***" Furthermore, since Geer also discloses that the invention uses smartcards, each of the parties in the embodiment where a business deal is conducted are presumed to use a smart card for maintaining the certificate and private key sent as also mentioned in col. 12, lines 30-37: "*The four enter the room and **insert their smart-card certifying authorities into readers** embedded in the desk in the room. **Crypto-secure channels to each of the participants' home systems are automatically constructed when the smart cards were presented.** The screens in the room light up to allow the participants to construct a conversation certificate to facilitate their work.*" For these reasons, Geer in view of Kanevsky teaches/suggests downloading a certificate and an associated private key to a token.

Appellants further contend, "Geer taken in view of Kanevsky does not teach or suggest searching for a match for the token ID and the user signature certificate in an authoritative database, and that a certificate and an associated private key are wrapped

with a public key associated with the token ID if a match is found for the token ID and the user signature certificate is found in the authoritative database." Examiner respectfully disagrees. Examiner would again, first like to note that a signature certificate, since not specifically defined, is nothing more than a certificate that contains a public key which can be used to verify a digital signature (see MPEP 2111). As discussed above, Geer teaches an embodiment of the invention for business deals using smart cards to facilitate authentication in col. 11, lines 40-52: "***Occasionally it will be necessary to add or delete a party to a conversation that is already under way. Upon receiving an instruction from one of the computers involved in the business deal to add or delete a party, the convener will create a new conversation certificate and distribute it to the new set of parties. The convener will record, as the final entry in a first message log, a link to a new message log and will record, as the first entry in the new message log, a link to the first message log, as described above in connection with FIGS. 3 and 4. The parties to the business deal may communicate using smart cards in personal digital assistants (PDAs), which might be wireless.***" Thus, Geer teaches that parties may be added to a conversation for a business deal, where a new conversation certificate must be created in order for that partner to gain access to the conversation. Geer also teaches that this method of conducting business is superior to the existing methods in col. 12, lines 6-13: "***The adoption of conversation certificates and introduction certificates as described above as a basic means of authorization by exchanges and other participants in the securities industry would enable the construction of new systems that would enable the***

construction of new systems that would 'systematize' a much broader range of business functions than is now possible. A much broader range of agency relationships will be supportable than is now the case. Since Geer did not explicitly disclose various elements, including that the token ID and user signature certificate must be searched for in an authoritative database and that the certificate and associated private key are wrapped by a public key associated with the token ID, Kanevsky was used to modify the transaction from Geer. Kanevsky suggests that a new user must have their smart card initialized/registered where a token identifier and a certificate are stored in a database so a user may be authenticated later in col. 7, line 51 – col. 8, line 4: ***"At the registration server 410, a system administrator typically inserts a new smartcard with his administrator smartcard and enters his PIN number to authorize the registration of a new user. The administrator then activates the user smartcard initialization program, which typically stamps the smartcard with information for a certificate such as user's private and public key set, user's names, serial number, smartcard serial number, etc. The registration server 410, which may be equivalent to workstation 220 of FIG. 3, creates the user profile, generates the request private/public key as well as the certificate, and downloads the information to the smartcard. Registration server 410 then requests the user to speak to the workstation speaker for identification purposes. These voice messages are sent to a speaker verification server 200, which is equivalent to ASSR server 200 discussed above with respect to FIGS. 1, 2 and 3. The voice messages, the certificate and the unique smartcard serial number are stored in a database***

associated with or incorporated in ASSR server 200 for future authentication and other uses. Kanevsky later suggests that the information, including a certificate and a token ID, are taken from the smart card and searched for in the ASSR server, where once the match is found the user is authenticated and a new PIN encrypted, i.e. wrapped, with a public key associated with the token ID in col. 8, lines 29-39: *"With his PC 450, user establishes connection with the ASSR server 200 via communication link L (through, e.g., SSL V2) to request his smartcard PIN change. Dialogue boxes or voice prompts are presented to the user to enter his user ID, name, smartcard serial number, etc. ASSR server 200 accesses the stored certificate and the user profile based on the entered information. ASSR server 200 then prompts the user to speak to the PC speaker with preset voice messages for authentication. The accessed user profile and voice segments from the database is compared with the input messages from the user for authentication. The user may be given a few chances to make correct inputs to the verification program. If the verification is correct and the user is a current valid user, the ASSR server 200 uses the smartcard certificates and public key to encrypt the PIN reset command and sends it to the user PC and the associated smartcard reader. The user smartcard then uses its unique private key to decrypt the RESET PIN command."* Examiner would also like to note that the term "associated" as used in the limitation "public key associated with the token ID" is broad and is therefore broadly interpreted to mean that the key is somehow associated with the smart card, i.e. token, which contains a token ID (See MPEP 2111). Thus, Kanevsky is used to modify Geer to add a level of authentication to the existing

steps a business entity must take to be added to a conversation. Using Kanevsky to modify Geer yields specific steps a business partner should take in order to be properly authenticated and introduced into the conversation by initializing the smart card.

Furthermore, although Kanevsky suggests returning a new PIN to the user, when modifying Geer, the new PIN is replaced with the new conversation certificate along with its associated private key. One would have been motivated to modify the method disclosed in Geer et al. with Kanevsky because doing so not only ensures that the information transmitted is both confidential and can only be decrypted by the user who has the private key associated with the public key of the smartcard, but also allows for a stronger means of authenticating each business partner before allowing that entity access to highly confidential information. Thus, Geer taken in view of Kanevsky teaches/suggests searching for a match for the token ID and the user signature certificate in an authoritative database, and that a certificate and an associated private key are wrapped with a public key associated with the token ID if a match is found for the token ID and the user signature certificate is found in the authoritative database.

In response to Appellant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Kanevsky adds a

stronger layer of authentication by not only requesting certain information (i.e. public/private key pair, certificate, smart card serial number, etc) included in the token, but additionally uses biometrics in order to ensure that the user is not an imposter in col. 8, lines 1-4: ***"The voice messages, the certificate and the unique smartcard serial number are stored in a database associated with or incorporated in ASSR server 200 for future authentication and other uses."*** Thus, the combination of Geer and Kanevsky result in a system which is more likely to prevent unauthorized users to gain access to confidential information. Furthermore, in response to Appellant's statement that "Geer does not even mention the employment of token IDs," Examiner would like to note that the term token ID is not specifically defined, thus for all purposes a token ID may even be interpreted (according to MPEP 2111) as the public/private key pair which is unique to each smart card disclosed in col. 2, lines 40-46: ***"The smart card 12 at authorizing computer 10 is initialized once by the creation of a public key pair for the smart card (a private key that never leaves the smart card and a public key that can be distributed to others) and a public key pair for the user of the card (a private key that the user keeps confidential and a public key that can be distributed to others)."*** Thus, the Examiner maintains that there is proper motivation to combine/modify Geer with Kanevsky.

Regarding Claims 2 and 10, 35 USC 103(a) Rejection:

Appellant contends "Geer in view of Kanevsky does not teach or suggest that a certificate and an associated private key is a plurality of certificates and associated private keys, wherein at least one of the certificates and associated private keys is a

signature certificate for a user, an encryption certificate for the user and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy.” Examiner respectfully disagrees. Geer teaches that one of the plurality of certificates is a role certificate which is associated with a private key for communicating with other entities that are active in that role and wherein the role certificate includes at least one policy, where the policy is specific to the authorizations that the role of being a business entity permits, in col. 4, line 61 – col. 5, line 6: “**Each authorization certificate in accordance with the present invention specifies membership in a ‘club’ that confers certain rights. Smart card owners would have the ability to confer membership privileges to other smart card owners, who would accumulate these membership privileges as authorization certificates stored in their smart cards. Because the authorization certificate carries a permission or authorization to perform a particular action rather than just an authentication of a person’s identity, the authorization relationships are inverted with respect to the conventional practice in connection with conventional public key identification certificates.**”

Furthermore, Geer teaches many other types of certificates that are used in the business embodiment where conversation certificates and the associated private key are also used for encrypting purposes in col. 9, lines 24-41: “Referring to FIG. 6, in operation of the system of FIG. 5, **each of the actual parties to the business deal obtains, from a certifying authority computer operated by an investment banking firm, an authorization certificate and a private key of a new public key pair minted by the certifying authority computer (step 78). The authorization certificate**

contains a description of the party's authority (shares controlled by the party, the right of the party to access certain files, and the right of the party to delegate authority to another party in the business deal, including DBA entities, or to an outside party). The authorization certificate also contains the public key of the new public key pair minted by the certifying authority computer as well as a hash signature, the time period during which the authorization remains valid, a serial number of the authorization certificate, etc. The authorization certificate is created by the certifying authority computer and used by the parties to the business deal in the manner described above in connection with FIGS. 1 and 2. Thus, Geer in view of Kanevsky teaches/suggests that a certificate and an associated private key is a plurality of certificates and associated private keys, wherein at least one of the certificates and associated private keys is a signature certificate for a user, an encryption certificate for the user and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy.

Regarding Claims 7 and 15, 35 USC 103(a) Rejection:

Appellants contend, "The teachings of Geer, Kanevsky, and Burn teach away from their combination and modification in the manner suggested by the Examiner, because the purported combination would result in an inoperable device." Examiner respectfully disagrees. In response to applicant's argument that these references teach away from one another, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or

Art Unit: 2137

all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). In this case, one would be motivated to modify the teachings of Geer in view of Kanevsky by Burn in order to incorporate yet another layer of security which is to require that a user enter a password before the operations may be performed as suggested by Burns in paragraph 6: ***"Passwords have also been used to protect automation accounts that are used to provide information or perform tasks. These 'robot accounts' that are routinely used to disseminate critical information to privileged employees and agents in large companies, governmental agencies, and other institutions. As such, automation accounts must be protected from compromise at all costs. In the present day, password protection mechanisms fall intolerably short of the security levels modern institutions demand."*** Although this passage seems to teach away based on the fact that it mentions passwords are not a strong form of authentication, in reality, the more types of authentication used within a system leads to a more secure system. True, if passwords alone are used, it is a weaker form of authentication, however passwords being used in addition to biometrics and a token storing certificate information definitely increases the security of confidential information. Thus, Examiner maintains that since the system is not only using passwords, and since passwords in addition to the two other forms of authentication taught/suggested by Geer and Kanevsky would strengthen the system, i.e. motivation for the combination, the teachings of Geer, Kanevsky, and Burn do not teach away from their combination and modification in the manner suggested

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

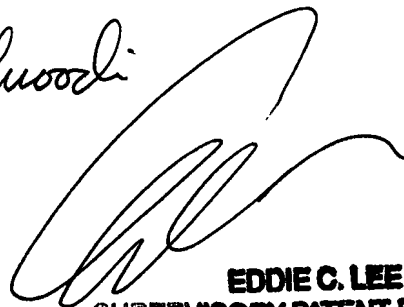
Respectfully submitted,

Nadia Khoshnoodi



Conferees

Eddie Lee



EDDIE C. LEE
SUPERVISORY PATENT EXAMINER

Emmanuel Moise

